What is claimed is:

1. A firewall system for protecting a network element from access over a network to which the network element is attached, the firewall system comprising:

a firewall box;

a first connection connecting the network to the firewall box;

a second connection connecting the firewall box to the network element; and

at least one proxy agent running on the firewall box for verifying that an access request packet received over the first connection is authorized to access the network element, the at least one proxy agent initiating a connection to the network element on behalf of the access request if the access request is authorized; wherein

the firewall box is a stand-alone computing platform.

2. The firewall system claimed in claim 1, wherein the firewall box is dedicated to a firewall application.

3. The firewall system claimed in claim 1, wherein the firewall box is a general purpose computer.

4. The firewall system claimed in claim 1, wherein the firewall application comprises a plurality of proxy agents, each of the plurality of proxy agents being individually suited, in accordance with a port number indicated in an incoming access request, for verifying the incoming access request.

5. The firewall system claimed in claim 1, wherein the at least one proxy agent verifies that a source address associated with an incoming access request is authorized to access the network element.

6. The firewall system claimed in claim 1, wherein the at least one proxy agent verifies that a user associated with an incoming access request is authorized to access the network element.

7. The firewall system claimed in claim 6, wherein the at least one proxy agent prompts the user to enter a user name and verifies the user name entered.

8. The firewall system claimed in claim 6, wherein the at least one proxy agent prompts the user to enter a user name and a password and verifies the user name and password entered.

9. The firewall system claimed in claim 8, wherein the at least one proxy agent, upon receiving and verifying the user name and password, communicates a second password to the user using an out-of-band means, which second password is to be entered by the user to advance a logon process.

10. The firewall system claimed in claim 9, wherein the second password is a random number.

11. The firewall system claimed in claim 9, wherein the out-of-bands means is a beeper.

12. The firewall system claimed in claim 1, wherein the at least one proxy agent verifies that a time period during which an incoming access request is received is valid.

13. The firewall system claimed in claim 1, wherein the at least one proxy agent verifies that an incoming access request contains no executable commands directed to the firewall box.

14. The firewall system claimed in claim 1, wherein the at least one proxy agent verifies that a destination associated with an incoming access request is valid.

15. The firewall system claimed in claim 14, wherein the at least one proxy agent verifies that a destination indicated an incoming access request is valid for a user associated with the incoming access request.

16. The firewall system claimed in claim 1, wherein the at least one proxy agent addresses the network element according to an alias.

17. The firewall system claimed in claim 1, wherein the at least one proxy agent manages the connection to the network element.

18. The firewall system claimed in claim 1, wherein the at least one ~~proxy agent operates in a daemon mode.~~

19. The firewall system claimed in claim 1, wherein the firewall system operates in a UNIX environment and the at least one proxy performs a Changeroot command prior to processing an incoming access request.

20. The firewall system claimed in claim 1, wherein an operating system of the firewall box performs packet filtering.

21. The firewall system claimed in claim 1, further comprising:

a router attached between the firewall box and the public network, which router performs packet filtering.

22. The firewall system of claim 1 ~~further~~ comprising:

a transaction log ~~for recording~~ information regarding an access request.

23. A firewall method for protecting a network element from unauthorized access over a network to which the network element is attached, the method comprising the steps of:

receiving an incoming access request; thereafter

assigning a proxy agent to the incoming access request in accordance with a port number indicated in the incoming access request; thereafter

verifying the authority of the incoming access request to access the protected network element by using the proxy agent as a verification means; and thereafter

using the proxy agent to form a connection to the network element on behalf of the incoming access request if the authority of the incoming access request is verified.

24. The firewall method claimed in claim 23, wherein an assigned proxy agent is selected from a plurality of proxy agents, each of the plurality of proxy agents being individually suited, in accordance with a port number indicated in an incoming access request, for verifying the incoming access request.

25. The firewall method claimed in claim 23, wherein the step of verifying the authority of the incoming access request includes:

using the at least one proxy agent to verify that a source address associated with an incoming access request is authorized to access the network element.

26. The firewall method claimed in claim 23, wherein the step of verifying the authority of the incoming access request includes:

using the at least one proxy agent to determine the identity of a source of the incoming access request;

using the at least one proxy agent to initiate a first set of verification checks in response to a first identified source; and

using the at least one proxy agent to initiate a second set of verification checks in response to a second identified source.

27. The firewall method claimed in claim 23, wherein the step of verifying the authority of the incoming access request includes:

using the at least on proxy agent to verify that a user associated with an incoming access request is authorized to access the network element.

28. The firewall method claimed in claim 27, wherein the method further comprises the steps of :

using the at least one proxy agent to prompt the user to enter a user name; and

verifying the authority of the user name entered.

29. The firewall method claimed in claim 27, wherein the method further comprises the steps of:

using the at least one proxy agent to prompt the user to enter a user name and a password; and

verifying the authority of the user name and password entered.

30. The firewall method claimed in claim 27, wherein the method further includes the steps of:

using the at least one proxy agent to communicate a second password to the user using an out-of-band means, which second password is to be entered by the user to advance a logon process.

31. The firewall method claimed in claim 30, wherein the second password is a random number.

32. The firewall method claimed in claim 30, wherein the out-of-bands means is a beeper.

33. The firewall method claimed in claim 23, wherein the method further comprises the step of:

using the at least one proxy agent to verify that a time period during which an incoming access request is received is valid.

34. The firewall method claimed in claim 23, wherein the step of verifying the authority of the incoming access request includes:

using the at least one proxy agent to verify that an incoming access request contains no executable commands.

35. The firewall method claimed in claim 23, wherein the step of verifying the authority of the incoming access request includes:

using the at least one proxy agent to verify that a destination associated with an incoming access request is valid.

36. The firewall method claimed in claim 23, wherein the step of verifying the authority of the incoming access request includes:

using the at least one proxy agent to verify that a destination indicated an incoming access request is valid for a user associated with the incoming access request.

37. The firewall method claimed in claim 23, wherein the step of using the proxy agent to form a connection to the network element on behalf of the incoming access request includes:

addressing the network element according to an alias.

38. The firewall method claimed in claim 23, wherein the at least one proxy agent operates in a daemon mode.

39. The firewall method claimed in claim 23, wherein the method is operates in a UNIX environment and the method further includes the step of:

having the at least one proxy perform a Changeroot command prior to processing an incoming access request.

40. The firewall method claimed in claim 23, wherein the method further includes the step of

performing packet filtering on the incoming access request.

41. The firewall method claimed in claim 23, further comprising the step of:

maintaining a transaction log for recording information regarding an access request.

42. A firewall system for protecting a network element from access over a network to which the network element is connected, the firewall system comprising:

means for receiving an access request from a source device over the network;

means for determining whether the source device is authorized to access the network element; and

means for establishing a connection to the network element on behalf of the source device in the event that the source device is authorized to access the network element;

wherein the firewall system runs on a stand alone computer connected between the network and the network element.

43. A firewall system as claimed in claim 42, wherein the determining means is a proxy agent assigned to the incoming access request, in accordance with a port number indicated in the access request, to verify the authority of the source device to access the network element.

44. A method for controlling a computer to act as a firewall for protecting a first network element from unauthorized access through a second network element over a network to which the first network element is attached, the method comprising the steps of:

receiving an access request to access the first network element at the computer;

assigning a proxy agent to the access request, based on a port number indicated within the access request, which proxy agent determines whether the first network element is authorized to access the second network element; and

using the proxy agent to establish a connection between the first and second network elements on behalf of the second network element if it is determined that the second network element is authorized to access the first network element.

45. A firewall process for operating a computer connected between a network and a network element to protect the network element from unauthorized access over the network, the firewall process comprising the steps of:

receiving an access request from a source device over the network;

determining whether the source device is authorized to access the network element; and

establishing a connection between the source device and the network element on behalf of the source device, if the source device is determined to be authorized.

46. An article of manufacture for use in a stand alone firewall computer to isolate a network element from unauthorized access over a network to which the network element is attached, comprising a computer usable medium having computer readable program code means for causing the computer to:

receive an incoming access request transmitted over the network;

assign a proxy agent to the incoming access request, which assignment is performed in accordance with a port number associated with the incoming access request;

use the proxy agent to determine whether the incoming access request is authorized to access the network element; and

use the proxy agent to establish a connection between the computer and the network element on behalf of the incoming access request if the incoming access request is determined to be authorized.